HIGHLY SECURE COMPUTER SYSTEM ARCHITECTURE FOR A HETEROGENEOUS CLIENT ENVIRONMENT

Field of the Invention

This invention relates to computer systems and more specifically to a secure computer system architecture for isolating heterogeneous client environments in the computer system.

Background

Powerful computer systems and software applications have become an essential and critical resource for many tasks such as large engineering and design projects. For example, electronic design and analysis (EDA) applications running on powerful computer systems allow engineers to design, simulate, and debug electrical circuits and circuit boards which are extraordinarily complex. Mechanical design and analysis (MDA) applications similarly allow engineers to design complex and reliable devices. However, design and analysis applications require very powerful computer systems with a great deal of memory, and the licenses to use the applications are extremely expensive. The design and analysis applications are also finely divided according to function, requiring designers to purchase license for

a large number of applications to complete an entire design project.

For example, an electrical engineering designer working on an electronic communication system may need to license individual EDA's for system level design, system verification, cabling design and analysis, printed circuit board design, printed circuit board analysis, printed circuit board layout, integrated circuit design, integrated circuit timing simulators, etc, with different versions for digital, analog, and RF portions of the communication system. Therefore, designers may spend millions of dollars acquiring and maintaining licenses for the essential design and analysis applications, and hundreds of thousands of dollars for the computer systems to run the applications. Managing computer and application resources to meet fluctuating requirements is a never ending struggle for large engineering firms.

In order to reduce the cost of licensing the design and analysis applications, some application vendors offer session-based licenses rather than time-based licenses, so that the designer is not paying for the application when it is not being used. Unfortunately, the designer still needs to maintain the expensive computer systems to run the application, even though the system is unused or lightly used much of the time.

Application service providers (ASP's) provide computer processing capability and applications for clients on an as-needed basis. The ASP acquires and maintains a large computer system and software licenses, and clients may process their data on the ASP's computer system and software applications. For example, various

ASP's may provide computer processing time and EDA's, MDA's, or other types of software as needed. The client can then either rely exclusively on the ASP to provide access to applications or can use the ASP to supplement their own resources during busy periods.

However, data security is of great concern to clients as they use ASP computer resources. Clients are typically concerned that other clients will be able to see, copy, or corrupt their data as it travels to or from or is processed on the ASP computer system. Clients may even process their data on the same ASP as their competitors, so data security is of utmost importance.

ASP's may protect client data by typical server environments which provide security through comprehensive access control lists, but they do not provide the physical isolation and encryption of the client data, nor do they provide the highest level of performance for many technical applications.

Consequently, a need exists for a highly secure computer system architecture for isolating heterogeneous client environments within the system.

Summary

To assist in achieving the aforementioned needs, the inventors have devised a highly secure computer system architecture in which client environments may be allocated as needed and which are isolated from each other. Secure environments are configured in portions of the secure computer system according to client needs. Each clients secure environment is isolated from other

clients environments. Clients may transfer data to and from the secure computer system across the Internet using a broadband or dial-up connection, or by direct connection, or by manual transportation of physical media as desired. Thus, the clients domains are effectively extended to include computer resources in the highly secure computer system.

A configuration engine in the highly secure computer system associates clients with computer resources. The configuration engine preferably receives resource allocation requests from clients and automatically configures the highly secure computer system to connect clients with requested computer resources. Alternatively, the configuration engine has a graphical user interface allowing an operator to configure the system manually.

The invention may comprise a method of providing a plurality of secure computer environments in a shared computer system. The method includes providing the shared computer system having a plurality of computers and at least one virtual local area network switch connected to the plurality of computers. A plurality of client connection ports is connected to the virtual local area network switch. A configuration engine is electrically connected to the at least one virtual local area network switch. The configuration engine includes computer readable program code for configuring the at least one virtual local area network switch. The configuration engine configures the at least one virtual local area network switch to connect each of the plurality of client connection ports to at least one of the plurality of computers while isolating the plurality

of client connection ports from one another. Each of the client connection ports may thus be connected to at least one of the plurality of secure computer environments on the plurality of computers.

The invention may also comprise a secure computer system having a plurality of computers, a plurality of client connection ports, and at least one virtual local area network switch. The at least one virtual local area network switch is electrically connected to the plurality of computers and to the plurality of client connection ports. The at least one virtual local area network switch is configurable to changeably connect each of the plurality of client connection ports to at least one of the plurality of computers while isolating the plurality of client connection ports from one another. A configuration engine is electrically connected to the at least one virtual local area network switch. The configuration engine includes computer readable program code for configuring the at least one virtual local area network switch to changeably connect each of the plurality of client connection ports to at least one of the plurality of computers while isolating the plurality of client connection ports from one another.

The invention may also comprise a secure computer system having a plurality of computers, a plurality of client data inputs, and means for securely connecting a portion of the plurality of client data inputs to a portion of the plurality of computers while isolating the portion of the plurality of computers from a second portion of the plurality of computers.

Brief Description of the Drawing

Illustrative and presently preferred embodiments of the invention are shown in the accompanying drawing, in which:

FIG. 1 is a diagram of a highly secure computer system with multiple clients connected to computer resources through a secure switched network;

FIG. 2 is a diagram of the highly secure computer system of FIG. 1 in which the secure switched network includes a virtual private network router and virtual local area network switches; and

FIG. 3 is a diagram of a highly secure computer system as in FIG. 2 including a configuration engine, a firewall and authentication software.

Description of the Preferred Embodiment

The drawing and description, in general, disclose a method of providing a plurality of secure computer environments in a shared computer system. The method includes providing the shared computer system having a plurality of computers and at least one virtual local area network switch connected to the plurality of computers. A plurality of client connection ports is connected to the virtual local area network switch. A configuration engine is electrically connected to the at least one virtual local area network switch. The configuration engine includes computer readable program code for configuring the at least one virtual local area network switch. The configuration engine configures the at least one virtual local area network switch to connect each of the plurality of client connection ports to at

least one of the plurality of computers while isolating the plurality of client connection ports from one another. Each of the client connection ports may thus be connected to at least one of the plurality of secure computer environments on the plurality of computers.

The drawing and description also disclose a secure computer system having a plurality of computers, a plurality of client connection ports, and at least one virtual local area network switch. The at least one virtual local area network switch is electrically connected to the plurality of computers and to the plurality of client connection ports. The at least one virtual local area network switch is configurable to changeably connect each of the plurality of client connection ports to at least one of the plurality of computers while isolating the plurality of client connection ports from one another. A configuration engine is electrically connected to the at least one virtual local area network switch. The configuration engine includes computer readable program code for configuring the at least one virtual local area network switch to changeably connect each of the plurality of client connection ports to at least one of the plurality of computers while isolating the plurality of client connection ports from one another.

The drawing and description also disclose a secure computer system having a plurality of computers, a plurality of client data inputs, and means for securely connecting a portion of the plurality of client data inputs to a portion of the plurality of computers while isolating the portion of the plurality of computers from a second portion of the plurality of computers.

A highly secure computer system 10 having multiple computers 12 may be used to provide various clients with concurrent access to computer resources such as data storage, data processing, or otherwise. For example, application service providers (ASPs) may use a highly secure computer system 10 to provide processor time and applications. Various client's computer systems 44, 46, and 50 may be connected to the highly secure computer system 10 by a broadband 14 or dial-up 16 connection across the Internet 20, or by a dedicated line 22, or by any other suitable data transmission means. A secure environment is established in the highly secure computer system 10 for each client, so that client data is protected from undesirable viewing, copying, or modification. The highly secure computer system 10 thus provides secure, accessible computer processing power and data storage for clients, reducing the cost of maintaining complex computer systems for the clients while ensuring that sufficient computer resources are available when needed.

Referring now to FIG. 1, a highly secure computer system 10 includes a group of computer resources 12 such as computer processors (e.g., 24 and 26) or storage devices, a secure switched network 40, and a configuration engine 42. The configuration engine 42 configures the secure switched network 40 to securely connect client computer systems 44, 46, and 50 to computer resources 12 as needed, while isolating each client's resources in the highly secure computer system 10 from one another.

In this exemplary preferred embodiment of the highly secure computer system 10, client A 44 has three local

computers 52, 54, and 56 connected to the Internet 20 through a router/firewall 60 across a broadband connection 14. Two computers 24 and 26 in the highly secure computer system 10 are connected to client A 44 through the secure switched network 40. Client A's domain 62 is thus effectively extended around the computers 24 and 26 in the highly secure computer system 10. Client B 46 has one local computer 64 connected to three computers 30, 32, and 34 in the highly secure computer system 10. The local computer 64 is connected to the secure switched network 40 across the Internet 20 using a dial-up connection 16, effectively extending client B's domain 66 around computers 30, 32, and 34 in the highly secure computer system 10. Client C 50 has one local computer 70 which is connected to one computer 36 in the highly secure computer system 10 across a dedicated line 22, such as a leased line. The local computer 70 is also connected through the secure switched network 40, effectively extending client C's domain 72 around the computer 70 in the highly secure computer system 10.

A configuration engine 42 in the highly secure computer system 10 configures the secure switched network 40 to securely connect the clients computer systems 44, 46, and 50 to computer resources 12 in the highly secure computer system 10. The configuration engine 42 preferably includes computer readable program code to be executed on a computer processor. The configuration engine 42 may include code 74 for automatically configuring the secure switched network 40 and code 76 providing a graphical user interface (GUI) for manual configuration of the secure switched network 40. The lowest level interface of the configuration engine 42 is

preferably a very simple single function command to associate clients with computer resources in the highly secure computer system 10. The GUI code 76 and the automating code 74 thus need only execute the single function command to configure the secure switched network 40. The automating code 74 in the configuration engine 42 may include load balancing systems or brokering systems which receive requests for computer resources 12 from clients and which automatically allocate resources 12 according to client need and priority, and resource availability.

The secure switched network 40, the configuration engine 42, and the computers 12 are preferably interconnected by a typical Ethernet with category 5 cables and Fast Ethernet network interface cards on the computers 12.

Referring now to FIG. 2, the secure switched network 40 in the highly secure computer system 10 may include at least one virtual private network (VPN) router 80 and a group of virtual local area network (VLAN) switches 82, 84, 86, and 90.

A virtual local area network may be implemented using many modern network switches such as the Catalyst series of network switches available from Cisco Systems, Inc. of San Jose, California. Such switches are described as "VLAN-capable." VLANs are typically used to limit network traffic to limited "broadcast domains" to improve performance. The VLAN switches 82, 84, 86, and 90 provide secure and isolated sub-networks in the highly secure computer system 10. A VLAN switch filters data by examining Internet Protocol (IP) addresses on data

packets and transmitting only those with recognized IP addresses.

The virtual private network router 80 encrypts data traveling across the network, providing a secure connection during transmission. Examples of VPN routers 80 include the Cisco 7140 VPN router, available from Cisco Systems, Inc. of San Jose, California, and the Compatible IntraPort 2+ VPN Access Server, available from Boulder, Colorado. VPN routers 80 are particularly useful for Internet connections such as the broadband connection 14 and dial-up connection 16. Direct connections such as the dedicated line 22 preferably also use the VPN router 80 in the highly secure computer system 10, although the VPN router 80 is not as critical with a dedicated line 22. A VPN router must be included at both ends of each link.

The clients 44, 46, and 50 are connected to the highly secure computer system 10 through client connection ports 92, 94, and 96 which are physical data ports in the highly secure computer system 10 or the secure switched network 40. All data entering or leaving the highly secure computer system 10, whether by the Internet connections 14 and 16 or direct connections 22, travel through the client connection ports 92, 94, and 96.

Client A 44 includes a VPN capable router/firewall 60 which encrypts outgoing data and filters and decrypts incoming data. Client A 44 is connected to a client connection port 92 in the highly secure computer system 10 over the Internet 20 on a broadband connection 14. The VNP router 80 receives and transmits data to client A

44 through the client connection port 92. The VNP router 80 decrypts data coming from client A 44 and encrypts data going to client A 44 so that the data is secure as it travels over the Internet 20. Thus, if the data is intercepted or monitored, the client's data is secure. Similarly, client B 46 and client C 50 include VPN routers 100 and 102, respectively.

The VLAN switches 82, 84, 86, and 90 connect the VPN router 80 in the highly secure computer system to the computer resources 12. VLAN switch 1 82 connects client A 44 to three computers 24, 26, and 30. VLAN switch 2 84 is unused in this example. VLAN switch 3 86 connects client B 46 to two computers 32 and 34. VLAN switch 4 90 connects client C to one computer 36. Note that client C 50 is connected to the highly secure computer system 10 on a dedicated line 22 rather than over the Internet 20, but is connected through the VPN router 80 to maximize security of client C's data in transit.

The VPN router 80 and VLAN switches 82, 84, 86, and 90 form the basis for securely extending the client's networking domains to include computer resources 12 in the highly secure computer system 10. Note that four VLAN switches 82, 84, 86, and 90 and one VPN router 80 are included in this example. However, practical implementations may have hundreds of simultaneous VLAN switches and a number of VPN routers.

The VLAN switches 82, 84, 86, and 90 in the secure switched network 40 are configured by the configuration engine 42. An exemplary sequence of configuration commands is given below, using the simple single function command mentioned above. This sequence may be generated

by the automating program code 74 or by a human administrator using the GUI code 76 in the configuration engine 42. The configuration commands configure the VLAN switches 82, 84, 86, and 90 to connect data ports so that information be transmitted between the ports recognized by the switch. Note that the ports can be physical ports (e.g., 110, 112, 114, 120, 122, and 126) located on the chassis of the VLAN switches 82, 84, 86, and 90 or virtual ports (e.g., 116, 124, and 130) which are defined in the VLAN switches 82, 84, 86, and 90 by ranges of incoming IP addresses. As the VPN connections with Clients allow limited IP address ranges, the VPN connections are effectively mapped to unique virtual ports on the VLAN switches 82, 84, 86, and 90 . Thus, the sequence to achieve the connectivity in FIG. 2 could be:

Add port 110 to VLAN 1 82
Add port 112 to VLAN 1 82
Add port 114 to VLAN 1 82
Add port 116 to VLAN 1 82
Add port 120 to VLAN 3 86
Add port 122 to VLAN 3 86
Add port 124 to VLAN 3 86
Add port 126 to VLAN 4 90
Add port 130 to VLAN 4 90

More detail will be given with respect to FIG. 3 below about designating the ports in the configuration commands. Once this configuration is complete the various clients 44, 46, and 50 will have access to their assigned computer resources 12 through the VPN router 80 and their VLAN switches 82, 86, and 90 but they will have no visibility of each others activities or data. Only devices connected through a VLAN switch 82, 84, 86, or 90

can communicate. For example, computers 24, 26, and 30 can share data through VLAN 1 82, as well as with client A 44, but no other clients (e.g., 46 and 50) or computer resources (e.g., 32, 34, and 36) will be able to communicate with the devices on VLAN 1 82.

Note that it is simple to make additional computer resources 12 available to a client 44, 46, or 50 by adding them to that client's assigned VLAN switch 82, 86, or 90, respectively.

Note also that FIG. 2 shows only the connections configured by the configuration engine 42. Other physical connections in the highly secure computer system 10 are not shown, but will be easily understood by those skilled in the art. Logical connections can only be established where a physical connection exists. Thus, each VLAN preferably has a physical connection to each computer resource 12. Various network topologies may be used to establish these physical connections without departing from the inventive concepts disclosed herein, therefore no further detail on the physical network connections between the VLAN switches 82, 84, 86, and 90 will be given.

Referring now to FIG. 3, another exemplary embodiment of a highly secure computer system 210 will be described. As before, three clients are connected to the highly secure computer system 210. Client A 244 includes three computer systems 252, 254, and 256, connected to the highly secure computer system 210 through a VPN capable router/firewall 260 over the Internet 220 on a broadband connection 214. Client B 246 has a single computer system connected to the highly secure computer

system 210 through a VPN router 300 over the Internet 220 on a dial-up connection 216. Client C 250 has a single computer system connected to the highly secure computer system 210 through a VPN router 302 on a dedicated line 222.

A secure switched network 240 in the highly secure computer system 210 connects the clients 244, 246, and 250 to computer resources 212 in the highly secure computer system 210. Data from the clients 244, 246, and 250 first passes through a firewall 330 in the secure switched network 240. The firewall 330 performs the standard functions of a firewall at the perimeter of a secure site, rejecting unauthorized network traffic by filtering out or passing data according to a set of filtering rules configured by the system administrator.

After the firewall 330 one or more VPN routers 280 and 332 are used to establish secure network connections with the remote client systems 252, 254, 256, 246, and 250. Each VPN connection is associated with one and only one client. Multiple VPN routers 280 and 332 may be useful to support a variety of remote client systems, various types of security (e.g., multiple encryption algorithms) or performance needs. VPN encryption functions may be included in routers, as in the exemplary embodiments herein, or in any other network devices.

An authentication function 334 is provided to verify the identity of the remote clients 244, 246, and 250 before the per-client VPN connections are established. The authentication function 334 verifies the identity of the clients 244, 246, and 250 before accepting data transfers from them, thereby preventing imposters from

accessing private data. There are several commercially available solutions for this function including SafeWord™ software, available from Secure Computing Corporation of San Jose, California. This software may be executed on the same computer processor as a configuration engine 242, or on a separate computer processor. Alternatively, the authentication function 334 may be embodied in a dedicated hardware device. The VPN routers 280 and 332 access the authentication function via a hardwired local area network (LAN) connection 336.

The VPN routers 280 and 332 decrypt encrypted network traffic from the clients 244, 246, and 250 based on this authentication information. After this decryption resulting network traffic is examined by the VPN routers 280 and 332 to verify that the specified destination IP address on the highly secure computer system 10 is valid for that specific client. Any IP address that doesn't pass this test is discarded. The mapping of clients 244, 246, and 250 to computer resource 12 IP addresses on the highly secure computer system 10 is maintained in a client to resource address map 340 in the configuration engine 242 and downloaded to the VPN routers 280 and 332 when the mapping changes.

At least one VLAN-capable switch 282 uniquely associates ranges of incoming IP addresses with a particular VLAN (where each client has a unique VLAN). Note that each VLAN may be processed by a separate VLAN switch 82, as in FIG. 2, or the VLAN's may all be processed in a single VLAN switch 282, as in FIG. 3. The data associating incoming IP addresses with a particular VLAN is kept in a client address to VLAN map 342 that is downloaded over a secure link to the VLAN switch 282

whenever the associations are changed. In addition, that VLAN is uniquely associated with a list of physical ports 310, 312, 314, 320, 322, and 326 on the VLAN switch 282 which are each connected to a single computer resource 224, 226, 230, 232, 234, and 236, respectively. These associations are kept in a VLAN to port map 344 in the configuration engine 242 and downloaded to the VLAN switch 282 when any changes are made.

Therefore, since each client 244, 246, and 250 is uniquely associated with a VPN router 280 or 332, that VPN router 280 or 332 is uniquely associated with a VLAN switch 282, that VLAN switch 282 is uniquely associated with a set of physical ports 310, 312, 314, 320, 322, and 326 on the VLAN switch 282 and those physical ports 310, 312, 314, 320, 322, and 326 are uniquely associated with individual computer resources 224, 226, 230, 232, 234, and 236, the client 244, 246, or 250 is uniquely associated with those computer resources 224, 226, 230, 232, 234, and 236.

The three maps (client to resource address map 340, client address to VLAN map 342, and VLAN to port map 344) in the configuration engine 242 are updated by a common piece of software that ensures that the tables are synchronized to eliminate any connections between clients 244, 246, or 250 and computer resources 212 that are not meant to be connected. For example, each time a map 340, 342, or 344 changes, the common software may verify each connection in the secure switched network 240 according to the maps 340, 342, and 344, removing unwanted connections that may be left over from previous configurations.

Alternatively, the common software may remove all connections in the secure switched network 240 and reconfigure the entire secure switched network 240 each time a map 340, 342, or 344 changes. However, this may cause disruptions to network traffic for clients whose computer resources 212 were not changed in the maps 340, 342, and 344.

The contents of the three maps 340, 342, and 344 in the configuration engine 242 are displayed in tables below, assuming the IP addresses shown in FIG. 3. Note this is only one exemplary way the information could be organized - many others are possible. The first table contains the client to resource address map 340, which specifies the mapping of clients (e.g., 244, 246, and 250) to computer resources 212 in the highly secure computer system 210. It is possible that a given computer resource (e.g., 212) may not be mapped to any client 244, 246, or 250 at a given time.

Resource IP Address	**Client IP Address**
10.10.10.1	20.15.100.1
10.10.10.2	20.15.100.1
10.10.10.3	20.15.100.1
10.10.10.4	53.4.100.6
10.10.10.5	53.4.100.6
10.10.10.6	90.5.7.6

The second table contains the client address to VLAN map 342, which specifies the mapping of VLAN number to client IP address. An example is shown below for the configuration shown in FIG. 2 (in which each VLAN was processed by a unique VLAN switch 82, 84, 86, and 90). Note that VLAN 2 (processed by VLAN switch 2 84) is not assigned to any client 44, 46, or 50 at this time.

VLAN Number	Client IP Address
1	20.15.100.1
2	
3	53.4.100.6
4	90.5.7.6

The third table contains the VLAN to port map 344, which specifies the mapping of the VLAN to physical ports on the VLAN switch 282. These ports might be specified is as a "blade" number and port on that blade, for example. In this example we assume the VLAN switch 282 supports two "blades" with 4 physical ports each. The computer resources 212 are connected to the physical ports as shown in FIG. 3.

Physical Port	VLAN
1,1	1
1,2	1
1,3	1
1,4	3
2,1	3
2,2	4
2,3	
2,4	

It is possible to represent this tabular data in many ways, or even combine the mappings into a single table. It is show here in three maps for clarity.

The highly secure computer system 10 and 210 described herein provides clients with a safe, convenient system for using shared computer resources. Each client is provided with a secure computer environment which can be initialized and configured according to the client's needs, in hardware, software, and operating system.

The highly secure computer system 10 and 210 also provides a safe and convenient way for a client to provide third party access to the client's data. If the client needs a third party to work on the client's data, both the client and the third party may be connected to the client's computer resources 12 and 212 in the highly secure computer system 10 and 210. For example, in a joint development project two remote clients may access the same client data in the secure computer system 10 and 210. A client may also need help debugging an EDA project. In this case, the software engineers who programmed the EDA software can be given access to the client's data so that they can debug the project in the actual working environment.

To provide this third party access, the VPN router (e.g., 280) in the highly secure computer system 210 to which the third party is connected is added to the configuration of the VLAN switch 282, as described above.

While illustrative and presently preferred embodiments of the invention have been described in detail herein, it is to be understood that the inventive concepts may be otherwise variously embodied and employed, and that the appended claims are intended to be construed to include such variations, except as limited by the prior art.